jamk.fi

# Cyber Security Incident Management Process in NOC/SOC Integration

## Master's thesis

Tanja Ruskojärvi

Master's Thesis
May 2020
Technology
Master's degree programme in Cybersecurity

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

**Description**

| Author(s)<br>Tanja Ruskojärvi | Type of publication<br>Master's Thesis | Date<br>11. May 2020 |
|---|---|---|
| | | Language of publication:<br>English |
| | Number of pages<br>45 | Permission for web publication: x |

Title of publication
Cyber Security Incident Management Process in NOC/SOC Integration

Degree programme
Cyber Security

Supervisor(s)
Lappalainen-Kajan, Tarja; Hautamäki, Jari

Assigned by
Erillisverkot Group

Abstract

Erillisverkot Group is a process organization, the operations of which are guided by processes. The organization's network operation center (NOC/SOC) has integrated network monitoring and security monitoring, mainly operating under the direction of the Incident Management Process. The importance of cyber security in incident management has grown significantly and Erillisverkot Group set the goal of implementing a separate Cyber Incident Management Process as part of the organization's process entity.

The production of the Cyber Incident Management Process began with an analysis of the current state, after which goals were set mirroring the organization's Security Strategy, and they include the requirements set by Risk Management. The process description took the laws and recommendations governing the organization's operations into account, as well as the service agreements made with customers. Based on these, the process description was created in accordance with JHS 152 recommendations.

During the process description, numerous detailed and case-specific work instructions were created, in addition, and as part of the process development, process indicators were defined, and based on them, reporting was created that is continuous. Process indicators and reporting serve as indicators within the organization and in the customer interface, informing e.g. about the service level and guiding the development of processes.

Upon completion of the draft process description, the process was tested under laboratory conditions. A test team of all the actors in the organization involved in the process participated in the testing. The reports generated from the testing were analyzed and the necessary corrections were made to improve the process. Once the completed as needed, the process was implemented as part of the organization's operations.

Keywords/tags:
Process organization, indident management process, cyber incident management process, JHS 152, ITIL, KATAKRI, Cyber security deviation, service restoration.

Miscellaneous

jamk.fi

**Kuvailulehti**

| Tekijät(t) | Julkaisun laji | Päivämäärä |
|---|---|---|
| Tanja Ruskojärvi | Opinnäytetyö, ylempi AMK | 11.5.2020 |
| | | Julkaisun kieli: Englanti |
| | Sivumäärä 45 | Verkkojulkaisulupa myönnetty: x |

Työn nimi
Cyber Security Incident Management Process in NOC/SOC Integration

Tutkinto-ohjelma
Cyber Security

Työn ohjaaja(t)
Tarja Lappalainen-Kajan, Jari Hautamäki

Toimeksiantaja(t)
Erillisverkot Oy

Tiivistelmä

Erillisverkot Oy on prosessiorganisaatio, jonka toimintaa ohjaavat prosessit. Organisaation verkko-operaatiokeskuksessa (NOC/SOC) toimii integroidusti verkonvalvonta ja turvallisuusvalvonta. NOC/SOC toimii pääsääntöisesti Tapahtumanhallintaprosessin ohjaamana. Kyberturvallisuuden merkitys tapahtumanhallinnassa on kasvanut merkittävästi, ja Erillisverkot Oy asetti tavoitteekseen erillisen Kybertapahtumanhallintaprosessin implementoinnin osaksi organisaation prosessipakkaa.

Kybertapahtumanhallintaprosessin tuottaminen aloitettiin nykytilan kartoituksella, jonka jälkeen asetettiin tavoitteet, jotka peilaavat organisaation turvallisuusstrategiaan ja sisältävät riskienhallinnan asettamat vaatimukset. Prosessikuvausta tehdessä otettiin huomioon organisaation toimintaa ohjaavat lait ja suositukset (mm. TUVE-laki ja KATAKRI) sekä asiakkaiden kanssa tehdyt palvelusopimukset. Näiden pohjalta luotiin prosessikuvaus JHS 152 -suositusta mukaillen.

Prosessikuvausta tehdessä syntyi lukuisia tarkentavia ja tapauskohtaisia työohjeita, lisäksi osana prosessikehitystä määriteltiin prosessin mittarit ja niiden pohjalta luotiin raportointi, joka on jatkuvaa. Prosessin mittarit ja raportointi toimivat indikaattorina organisaation sisällä ja asiakasrajapinnassa kertoen mm. palvelutasosta ja ohjaavat prosessien kehitystyössä.

Prosessikuvauksen luonnoksen valmistuttua prosessia testattiin laboratorio-olosuhteissa. Testaukseen osallistui kaikista prosessissa mukana olleista organisaation toimijoista koottu testiryhmä. Testauksen perusteella syntyneet raportit analysoitiin ja niiden perusteella suoritettiin tarvittavat korjaukset prosessin kehittämiseksi. Kun prosessi oli täydennetty tarvittavilta osin, se jalkautettiin osaksi organisaation toimintaa.

Avainsanat
Prosessiorganisaatio, tapahtumanhallintaprosessi, kybertapahtumanhallintaprosessi, JHS 152, ITIL, KATAKRI, kyberturvallisuuspoikkeama, palvelun palautus.

Muut tiedot

# Contents

# 1 Introduction

"There are only two types of companies: Those that have been hacked, and those that will be." Today it is not a question about "if" a company will be attacked but "when" and "how often" cyber attackers will attack a company. (Mueller 2012.)

Today companies operate by using several information systems, which somehow trust security. Security is indeed an extensive abstract that carries all different technologies; the environment where those technologies operate, transmission systems that transport the information between technologies, locations, and people who operate with all these mentioned components. Despite the raising awareness of rapidly increasing cyber threats, several companies remain unprepared to deal with them.

This Master's Thesis is assigned by a governmental organization Erillisverkot Group. It presents a report about generating a cyber security incident management process, testing that specific process in a laboratory environment and creating a plan for continuous development of the process. The main goal is to increase and ensure the security overall through the incident management process by, considering all the components using that particular process.

# 2 Research Plan for generating Cyber Security Incident Management Process

## 2.1 Goals

The goal is to generate as functional processes and procedures as possible to Erillisverkot Group, so that Erillisverkot Group will achieve a sufficient capability to respond to cyber incidents. After the processes are generated and described, they will be tested at a laboratory environment in order to find any lack of processes. After testing and reporting, the processes will be developed for further use as cyber incident response methods in Erillisverkot Group. Another goal is to find out and define the indicators Erillisverkot Group needs to measure in production regarding

the cyber incident management. One important goal is to identify the sufficient resources Erillisverkot Group needs for implementing this particular process into production. In order to assess the resources, it is important to take into account the continuous development of the process and mobilize it into organization.

## 2.2 Introduction of research problem

The main problem is how Erillisverkot Group can response to cyber incidents in the most efficient way and which are the procedures and operations needed to execute when preventing or at least mitigating the effects of cyber incidents when they occur, so that the influences can be minimized. The problem is also how Erillisverkot Group can restore services when deviation generates despite of protective.

There are three important issues to take into consideration when improving the cyber incident response in the organization. The first is that every employee of the organization understands the overall structure of the company, the big picture, so that all employees know the access to resources, what and where to find them and who to contact after a cyber incident has been discovered. Due to a lack of understanding of what has happened causes delay in response time and the increasing amount of time can cause increasing of devastation cyber incident causes. (Groppe 2019.)

In the NOC/SOC where this Cyber Security Management Process is about to be implemented, it is important that every supervisor working at NOC/SOC is aware of the location where to find the instructions when a cyber incident occurs, so that every step after that is clear and the methods are appropriate and logical, i.e. the Cyber Incident Management Process is described, and all the procedures are possible to execute so that the delays between the appearance of cyber incident and response for it are as short as prossible. That time is called a reaction time and will be one of the meters of this process, which is necessary to measure for finding out the possible reasons that increase the reaction time.

The second important issue for Cyber Security Incident Management is to involve the organization's legal team when the discovered incident has occurred. When a cyber

incident exceeds the threshold of reporting about it to governmental entities, the legal team ensures that it will be reported appropriately. (Groppe 2019.)

The third issue is about strategical communication. All employees of the organization should have awareness about information sharing policies and procedures concerning it. Too often employee have fear of reporting a potential attack internally, which can be barrier for developing an effective incident management. Especially when cyber incident has a significant or wide spread impact, it is important that all empoloyees of the organization understand how to respond and decrease the impacts of incident, and that will take place only if communication inside the organization is enough open and sufficient. (Groppe 2019.)

## 2.3 Plan for solving the problem

This Master's Thesis is limited physically to regard the department of Erillisverkot Group, that is responsible for network operating systems and network monitoring (NOC/SOC), and it concerns specifically this department's functionalities and processes (Incident Management Process). This research does not editorialize other processes of Erillisverkot Group; its focus is particularly on Cyber Incident Management and any issues regarding it.

The master plan is at first to describe the Cyber Incident Management Process in theory level by planning a flowchart (MS Visio) indicating the main steps of the process. After that, it is necessary to produce more specific, written technical instructions (MS Word) for all steps of flowchart. At this stage of the research, all resources regarding the owner of the process must be defined, as well as all roles, systems and, stakeholders, needed for process.

The final result of this Master's Thesis is Cyber Incident Management Process, which includes procedures, operations, restoration plans and all necessary components for the management of cyber incidents in Erillisverkot Group. In addition, this Master's Thesis is about to find out necessary meters needed for measuring Cyber Incident Management Process continuously to develop it as it is needed.

# 3 Theory part

The theoretic background of the research is introduced in this part. An overview of the main concepts commonly used in this Master's Thesis is intorduced. The second chapter presents the technologies and systems used in Erillisverkot Group and in this research as well for that reason. The last chapter concentrates on contracts and instructions, which obligate Erillisverkot Group. All this creates the frameworks and guidelines for the research, and they are based on strategies of the organization.

The source of information is ITIL, formerly an acronym for Information Technology Infrastructure Library, which is a set of detailed practices for IT service management, as well as, the auditing tools (Katakri, Vahti) and different instructions and guidances generated by Erillisverkot Group. Other important sources of information are customer requirements and contracts (SLA) as well as different kinds of publications concerning Incident Management, cyber security, threat protecting, risk management, deviation restoration, and abstracts including cyber incident management.

## 3.1 Overview of main concepts

Common and most important concepts used in this research are process, process oriented (organization), sub-process, procedures, work instructions, cyber security, deviation, incident management, service restore, information security, flow chart, classification and meters of measurements of the Cyber Security Incident Management Process.

### 3.1.1 Process-oriented organization

Tinnilä and Laamanen (2009, 121) have defined process as a series of acts linked to each other, and these acts create the output from the input by using the resources process is required. The main goal of process management is to create and form the

most competent procedures for the process that the input would be reached as cost-efficiently as possible.

Cyber Security Incident Management Process is generated for Erillisverkot Group, which is a so called process-oriented organization. That means almost all the action and services Erillisverkot Group produces are based on some certain and described processes. For that reason, employees doing their work duties are mostly led by the processes instead of people in charge, i.e. the processes are directing the activity. However, Erillisverkot Group is not purely process-oriented and functional elements are defining the activity. The structure of management in Erillisverkot Group is referred to as a matrix form of organization, which is described in Figure 1. That is why Erillisverkot Group has two types of managers, who have different roles in the the organization; line managers and process managers. The so called line managers are responsible for administrative affairs, and the process managers are responsible for processes put into practice. Process managers are also the owners of specific process named to each process manager.


Figure 1. Structure of management in Erillisverkot Group

Erillisverkot Group uses four main processes, which are divided into sub-processes. This research focuses on the sub-process Cyber Incident Management Process, which

is part of one of the main processes, namely Maintenance of Network and Services. Other main processes, not surveyed in this research are Management of Customership and Services, Management of Service Platform Lifecycle and Management of Construction and Shipments.

Maintenance of Network and Services Process is divided further into three sub-processes, which are Incident Management Process, Change Management Process and Problem Management Process. This research is about to produce one new sub-process under it, Cyber Incident Management Process.

### 3.1.2 Incident Management Process

In this certain Erillisverkot Group, for which this research is produced, Incident Management Process is used for responding to service disruptions and service restoring as a part of high quality of services. ITIL Service Operation defines Incident as "an unplanned interruption to a service or reduction in the quality of a service" (ITIL 4 edition Glossary 2019).

Incident Management Process starts when a certain input occurs in the process. In Erillisverkot Group this input can occur when customer reports an issue or from monitoring system as an alarm. After that the operator who works as a resource of the process collects as much information as necessary, and different types of incidents are categorized and prioritized regarding on this collected information. That part of the process produces a ticket from the input, which is appropriately categorized and prioritized, and it will be entered into the system. Categorization and prioritization ensure that the ticket will be routed as it is described in Incident Management Process Description, which in turn is based on Service Level Agreements (SLA).

Once the ticket has entered the system, a proper specialist provides the resolution for the issue and closes the ticket after it has been diagnosed in an analysis. In case, the so-called level 1 specialist cannot solve the issue, the ticket will be escalated to the next level (level 2 specialist). Escalation is an option as well if the impacts exceed the limit set to SLA levels. The latter escalation means that a certain incident is

communicated to the higher level of management, all way up to highest authorities if necessary. All the actions carried out during that chain of proceeding the incident are described in Incident Management Process which guides the proper procedures so that the input reaches the final resolution. These procedures include all activities needed for service restoration, as well as actions that are to be performed if the impacts are major or critical.

Lifecycle of incident can be summarized as follows: (Manage Engine 2019)

Step 1: Incident logging.
Step 2: Incident categorization.
Step 3: Incident prioritization.
Step 4: Incident assignment.
Step 5: Task creation and management.
Step 6: SLA management and escalation.
Step 7: Incident resolution.
Step 8: Incident closure.

Prioritization of an incident has four classes, and it is calculated after the impact and urgency have been defined by a relevant specialist operating the particular incident. The impact represents the level of damage the issue causes, and the urgency indicates the time within which the incident should be resolved. The system determines priority as a function of its impact and urgency using a priority matrix automatically, those priority categorizations are low, medium, high and critical. (Manage Engine 2019.)

When an incident is resolved with the actions the specialist(s) have made, it is considered as Incident resolution stage. After the customers have acknowledged the resolution and they are satisfied with it, the incident will be closed. (Manage Engine 2019.)

Once the incident has been closed, it is documented and analyzed if necessary for later use. In addition, regular reporting helps to maintain awareness of situation as well as further development and evaluation of Incident Management Process since the product of documenting will as well produce and increase a solution database.

### 3.1.3 Cyber Security Deviation

NIST, an acronym for National Institute of Standards and Technology, is an agency under the United States Department of Commerce tasked with promoting innovation and standards. NIST Institute was founded in 1901. (NIST History 2020.) NIST has created the Framework for Improving Critical Infrastructure Cybersecurity 1.0 in 2014, and version 1.1 was released in 2018, replacing the version 1.0. That risk-based Cybersecurity Framework (CSF) is the result of the Executive Order "Improving Critical Infrastructure Cybersecurity", which was established by the President of the United States on February 12, 2013. The Framework focuses on guiding cybersecurity activities and taking cybersecurity risks into account as a part of an organization's risk management process. The Framework allows organizations to apply the risk management principles and best practices to improve the security and resilience of critical infrastructure. The Framework can be applied regardless of the size of the organization, the degree of cyber security risk, or how sophisticated the cybersecurity is in the onrganization. There are three parts in the Framework: the Core, the Profile, and the Implementation Tiers (Framework for Improving Critical Infrastructure Cybersecurity 2018.)

The CSF maturity model is based on organizational self-assessment and is designed to help organizations cost-effectively identify, assess, and manage risks relatetd to the cyber environment. NIST encourages organizations to customize the model as needed to maximize its benefits. The Framework is not intended to be ready-made and universal model that works for everyone. Its purpose is to help the organization develop its own approach to cybersecurity, so that the requirements, threats, risks, vulnerabilities and resilience specific to the organization are taken into account as effectively as possible. The Framework aims to reduce and manage risks. (Framework for Improving Critical Infrastructure Cybersecurity 2018.)

The Framework consists of three components: the core of the framework, the implementation rates and the profiles of the framework. The frame of reference consists of a set of cybersecurity activities, desired customers, and applicable references that are common in various industries. The frame of reference guides the organization to develop its own cybersecurity profile. It can be used to prioritize

measures, risk tolerance and resources. The kernel contains five evaluable functionailities: identify, protect, detect, respond, and recover as seen in Figure 2. (NIST Cyber Security Framework 2020.)


Figure 2. Cybersecurity Framework version 1.1

Functionalities are divided into categories, subcategories, and information references. These are designed to help an organization achieve its cybersecurity goals. Looking at all five functionalities together provides a strategic perspective on managing an organization's cybersecurity risks. (Framework for Improving Critical Infrastructure Cybersecurity 2018.)

## 3.2 Overview of BMC Remedy

The main system used in this research is the system used for management of work in Erillisverkot Group which highly follows ITIL (Information Technology Infrastructure Library). This service management system is BMC Remedy and it provides incident management in addition to all other managements the Organization mostly uses and these are change, releasement and problem management.

The BMC Remedy is a service management software that provides practices that are in alignment with ITIL principles. BMC Remedy is a software offered by an American corporation BMC Software Inc. BMC has years of experience in IT management, which e.g. has been recognized as the Director of ITSM Gartner Magic Quadrant for the next six years. BMC markets itself by announcing on its website that it produces solutions that provide speed, agility and efficiency to meet business challenges in the areas of service management, automation, operations and central processing. (BMC Corporate 2020.) According to BMC Corporation, they offer people-centric solutions that effectively exploit modern technologies such as artificial intelligence (AI) and machine learning. The BMC Remedy product features include proactive service management through automatic incident classification, assignment and routing, where embedded features of multiple networks transmit incidents, changes and announcements between service providers. According to the manufacturer, this system also offers an integration with leading agile tools such as Jira, as well as cognitive e-mail analysis and automated actions on behalf of the user. (BMC IT-solutions 2020.)

The BMC Remedy system includes several different consoles for service management which are listed below:

- Incident Management
- Problem Management
- Knowledge Management
- Service Management
- Change Management
- Release Management
- Asset Management
- Configuration Management
- Service Request
- Service Level Management

Incidents can be created and resolved fast with intelligent, context-aware and proactive matching of incidents so that direct visibility into corporation's priorities is achieved through CMDB integration. Incident Management integrates all IT service support functions including change, asset, service level, service request, identity and information management. With intelligent and multi-channel self-service, it is possible to achieve lower call volumes and expert services through the BMC Workplace service, and comprehensive training and ready-made ITIL processes are also available. (BMC IT-solutions 2020.)

Knowledge management brings the key information to customers and supports employees by built-in Knowledge Centered Services (KCS). KCS supports to the delivery of services quickly and accurately. Knowledge Management enables the lifecycle management of information articles and ensures that up-to-date information is obtained throughout the organization. Problem solving is aided by bringing information from multiple and separate sources into the system through external information integration. Change Management manages the documentation of changes and the coordination of change requests throughout the IT environment of the corporation - from data centers to the desktops. Release management is used for combining several changes into a single release and allows manager to manage all related activitieds to support a successful release. Release Management informs stakeholders automatically as the publishing process progresses and, which can also be used to optimize the costs of the changes and minimize the potential for risks by a fast deliver of changes. (BMC IT-solutions 2020.)

BMC Remedy system also includes a powerful report tool, which provides 90 out-of-the-box reports to get quickly started and there is a possibility to create custom reports and dashboards. Storyboard offers the feature to generate slide shows with efficient report data. The reporting tool makes it possible to share and gain insights through collaboration features, as well as get automated information based on the relevance of the data. (BMC IT-solutions 2020.)

## 3.3 Overview of contracts, instructions and guidelines

Erillisverkot Group is a public entirely state-owned special-purpose organization headed by the Ministry of Finance. Therefore, all the functions and operations of Erillisverkot Group are led by government regulations. In addition, many guidance, instructions and contracts made inside Erillisverkot Group (internal) as well as instructions and contracts made with cooperators of the organization (external) define the way how Erillisverkot Group operates. This part contains a summary of principles that govern Erillisverkot Group and Cyber Incident Management Process will be generated based on these. (Erillisverkot Group 2020.)

### 3.3.1 JHS 152

JHS is Pubic Administration Recommendations generated by the Advisory Committee on Information Management in Public Administration (JUHTA - Julkisen hallinnon tietohallinnon neuvottelukunta. (The Advisory Committee on Information Management in Public Administration 2010.) This research concentrates on JHS 152 recommendation, the purpose of which is to standardize and clarify the description of processes in public administration. The baseline in developing processes is the strategy and vision of the organizations including all principles concerning functionalities of them. Process descriptions are the tool for managing, administrating and improving processes. In addition, process descriptions are used for induction and orientation regarding new employee as well as education and development of information management systems. (JHS-Public Administration Recommendations 2012.)

In JHS 152 recommendation the processes are divided into four levels of description which are process map, operating model, process path and workflow. The level of details concerning descriptions increases while the description goes further, level by level. Object Management Group's (OMG) Business Process Modeling Notation (BPMN) is applied to modelling. It defines the symbols used in the description. Users of JHS 152 recommendation are all public sector actors whose work consists of writing process descriptions. (JHS-Public Administration Recommendations 2012.)

### 3.3.2 Katakri

Finnish National Security Auditing Criteria Katakri is an auditing tool for authorities which is used when the organization's ability to protect classified information must be evaluated. The minimum requirements concerning international legislation and obligations are composed into Katakri, and the requirements documented in Katakri are divided into four fields, which are security management, personnel security, physical security and technical information security. Katakri can be used as an audit tool when evaluating a company's security arrangements and the safety of authorities' information systems. (Valtioneuvoston artikkeli 2015.)

The first Katakri was completed in 2009 as a part of an internal security program of the Finnish Government and the Katakri was first updated in 2011. The coordinator of Katakri renewal is a steering group which operates under National Security Agency (NSA) cooperation workgroup. Katakri is approved for use by the cooperation workgroup of NSA on 26 March 2015. (Valtioneuvoston artikkeli 2015.)

An example presented in Katakri II procedure of security audit includes nine functional steps shown in Figure 3. The first function is recognition of the company's need for Facility Security Clearance (FSC). After the need for an audit has been identified, the second function is to define the classification level (levels IV – II), and a general image of the target to be audited can be built based on that (Function 3). The fourth function includes processes as an audit team goes through the company's security documentation, and the security assessment is based on these revelations. Once the assessments have been carried out comments of fatal deficiencies of findings can be made if necessary. Hence, this is an optional function. After these functions it is time for the first audit (Function 6) and a report of that audit (Function 7). These two functions will be repeated until the FSC is approved (Function 9). (KATAKRI version II 2011.)

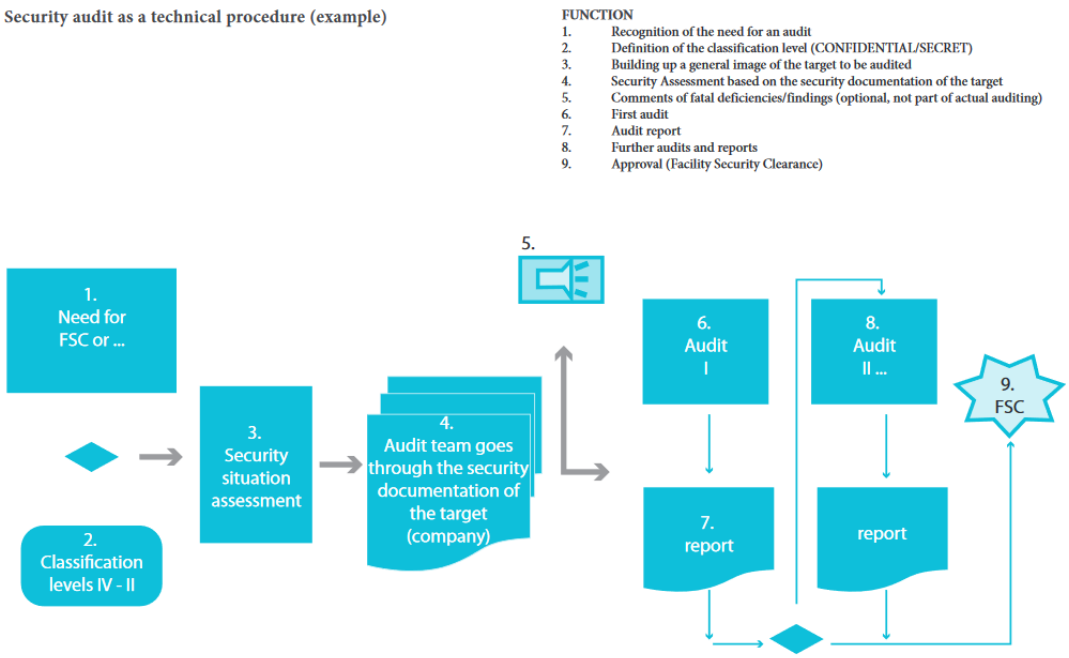


Figure 3. Example of security audit

As mentioned before, Katakri is divided into four main fields. Each of these fields is based on tripartite classification of requirements regarding security: the base level (level IV), the increased level (level III) and the high level (level II). The main goal of the part which defines the criteria of security management is to ensure that a company has sufficient preparedness and capability concerning administrative security. That part of Katakri describes the basis level a company must reach considering security management. In the part that defining physical security requirements, the requirements of physical environment are described where the classified information is processed. These environments are divided into three safety categories based on the need of processing and storing classified information, which are administrative area, safety area and technical safety area. Regarding the part about technical information security, Katakri describes the security requirements for technical information processing environment. All these guidelines are described and there can be several ways to execute the criteria. (KATAKRI version II 2011.)

# 4 Action Part

This part is describes how Cyber Security Incident Management Process was generated. The research execution included the steps listed below:

1. Analyzing the present state and creating the model of what requirements Erillisverkot Group has what comes to Cyber Security Incident Management Process.
2. Creating the draft of process (flow chart and detailed commentary of procedures).
3. Reviewing the draft with main operators of the process and complete and/or fix the draft if needed.
4. Testing the process in laboratory environment.
5. Final completions and fixing based on demonstration.
6. Measuring and reporting the results.
7. Implementation.

## 4.1 Analysis of Present state and needs of Cyber Security Incident Management Process in Erillisverkot Group

The first step while executing the research was analyzing the present state of Erillisverkot Group. The main point was that there was an existing Incident Management Process which editorializes some parts what regarding cyber incidents. An increasing need to protect the network of Erillisverkot Group while cyber threats are growing day after day was the main reason why Erillisverkot Group required the process planned specifically if and when cyber incidents occur. The truth was that the existing Incident Management Process would not be sufficient and precise enough in order to prepare, defend and recover from an event should something happen. Another point was that because the Incident Management Process did not editorialize appropriately if any cyber incidents occur, so proper indicators where needed to discover if so called normal traffic chances and particular thresholds surpasses. A custom-made process with proper indicators adduces immediately if normal traffic chances somehow, or if malicious traffic occurs. In addition, Erillisverkot Group had a need to produce reports of cyber incidents as well as it already reports of all other network incidents as an aim to develop Erillisverkot Group's action in the whole environment it operates in.

Erillisverkot Group produces ICT solutions for Finnish public authorities and critical operations of national security. For that reason, Erillisverkot Group offers overall

security and safety which considers almost everyone in Finland. Hence; it is especially very important that the quality of service is practically aimed to be 100%, 24/7/365, every day of the year. For all practical purposes this means continuous development and evaluation of processes and for all purposes the Cyber Incident Management Process was needed to ensure all this comprehensive.

### 4.1.1 Risk Management

Data collection started two years ago in spring 2018 and the final data collection was ready in April 2019. This data included material from other processes used in Erillisverkot Group, for example the Risk Management Process. One important matter was to define resources available to the Cyber Incident Management Process, including the employees operating with that particular process as well. One ambition during the present state analysis was to define the risks threatening Erillisverkot Group. In this case, the risks were categorized as cyber threats, which indeed is an extensive concept. Risk management itself is left out of this research for the reason that it is its own entire process including continuous identifying and responding to the risks. This research concentrates only on the risks that are categorized as cyber risks. These risks were assessed in close cooperation with the Risk Management Process manager and defined the cyber risks are seen in Table 1.

Table 1. Risk Management Table

| RISK MANAGEMENT TABLE | | | | | | |
|---|---|---|---|---|---|---|
| THREAT AGENT | RISK | ASSET | VALUE OF RISK (0-5) | SECURITY CONTROLL | THE RISK AFTER | ORGANIZATION AND PROGRESS |
| Human, Technological | Subcontractor leaks information | Information | 4 | Audit subcontractor from time to time | 2 | Security governance, Security policy |
| Human, Environmental | Accidental cable fault | Network, Signal station, Fiber | 3 | Readiness unit | 2 | Environment safety |
| Human, Technological | Breaking equipment | Network, Signal station, Fiber, Information | 4 | Reserve equipment, Backups, Readiness unit, Planning | 3 | Anticipation |
| Enviromental | Power failure because of electric storm or falling trees. | Network, Signal station, Fiber, Information | 4 | Backup power supply,Readiness unit | 3 | Environmental safety, anticipation |
| Human, Technological | Eavesdropping, Information leaks, gets stolen and or corrupts | Network, Signal station, Fiber, Information, Key personnel | 2 | Education of emplyees, Seurity management, Audit | 2 | Security governance, Security policy, Environment safety, Continuity management |
| Human | Third party hires employee | Key personnel, Information | 4 | Ascending career, Change | 2 | Security governance, Continuity management |
| Human, Technological | Accidental misconfiguration | Network, Signal station, Information | 3 | Managed documentation policy | 2 | Security policy |
| Technological | Climate control breaks | Network, Signal station | 2 | Controlled management system | 1 | Security governance |
| Human, Technological, Environmental | Physical entry to secure location by unauthorizes personnel | Signal station, Information | 5 | Premise security, Electrical physical access control | 3 | Security policy, Crime security |
| Human, Technological | Humint | Key personnel, Information | 2 | Information segmentation. | 2 | Security governance |
| Human, Technological | Denial of service | Information, network | 3 | Outside access limited to frontline servers only | 1 | Security governance, Security policy, Crime security, Foreign operation security |

The risk management table shows an evaluation of essential risks for Erillisverkot Group bound to an asset that the risk belongs to. The risk has been given a risk value (0-5) that shows the importance of the risk in relation to the hazard. A security control has been set to manage the risk level to a sufficient level.

This Risk Management Table provided the framework for what kind of threats Erillisverkot Group has to recognize and how to process those threats in the BMC Remedy system. The baseline of Erillisverkot Group's safety strategy is to identify threats when preventing all its elements from getting corrupted. In addition, one goal is to prevent unauthorized disclosure of Classified Information in all the environments, where it is processed. Erillisverkot Group has Threat Management for that process, which defines external and internal threats directed to an organization.

### 4.1.2 Threat Management

The baseline of Erillisverkot Group's Safety Strategy is to identify threats when preventing the network and all its elements from getting corrupted. In addition, one goal is to prevent unauthorized disclosure of Classified Information in all the environments, where it is processed. Erillisverkot Group has Threat Management for that process, for defining external and internal threats directed to the organization.

A threat source can be internal, external or both. Internal threats occur when someone has authorized access to the network and system with either an account on a server or physical access to the network and system.

External threats come from individuals or organizations working outside of an authorized party. External threats do not have a direct access to the computer systems or network. These external attacks occur through connected networks, physical intrusion, or from authorized partner networks.

Threat agent is the actor that imposes a threat to the system. The three main identified agents are human, environmental and technological agents. A human threat can be an insider or outsider.

An insider can have an indirect effect on the information and its systems that are accidental and non-malicious. An example of an employee's action or failure is an action against the organization's process, or just an accident where an employee works on cablework and detaches the wrong cable or accesses unauthorized information without appropriate purpose.

An insider or outsider can also have direct intentional and malicious effects. An example is a resentful employee who has agenda to destroy, corrupt or steal information or an outsider who has some reason to harm the organization, or who just wants to steal information to gain something.

An outsider can also have influence by mistake, e.g. by hiring key personnel without knowing the effects on the authority or subcontractor can cause something without knowing what or where he or she is doing and breaks fibre cables.

Environmental threats are caused by a non-human agent, nature based elements such as animals and changes in weather conditions. The most obvious external threats to ICT systems and the information are environmental, e.g. fires, floods, winds, falling trees, lightning storms and even in some cases solar flares. Other threats are terrorist attacks and wars.

Technological threats are caused by physical and chemical processes on the material. This includes all the equipment on the system and its life expectation.

All these threats harm the system even accidentally, indirectly and non-maliciously or intentionally, directly and maliciously, and the risk of each of them has been calculated based on the impact and urgency value given in the BMC Remedy.

## 4.2 Generating and reviewing the draft of the process

The Cyber Security Incident Management Process is based on JHS 152 recommendation, which standardizes and clarifies the description of processes in public administration. The risk survey and threat analysis provided the picture of possible incidents which may occur in the environment of Erillisverkot Group. The

next step was to plan how to identify, protect, detect, response and recover from each kind of cyber incidents referring to NIST Cybersecurity Framework.

The Cyber Security Incident starts when the input (cyber incident) occurs, which means it has already been identified, and somehow it has been impossible to detect it. That means the next stage is to respond to it. All the steps after the input has come into process have to be described as accurately as possible, so that the goal can be reached and the output is as required. The goal is to reach back the level where no cyber incidents can affect Erillisverkot Group or its functions as well as services it produces. That is the so called normal level. The flow chart of the Cyber Security Incident Management process is shown in Figure 4.

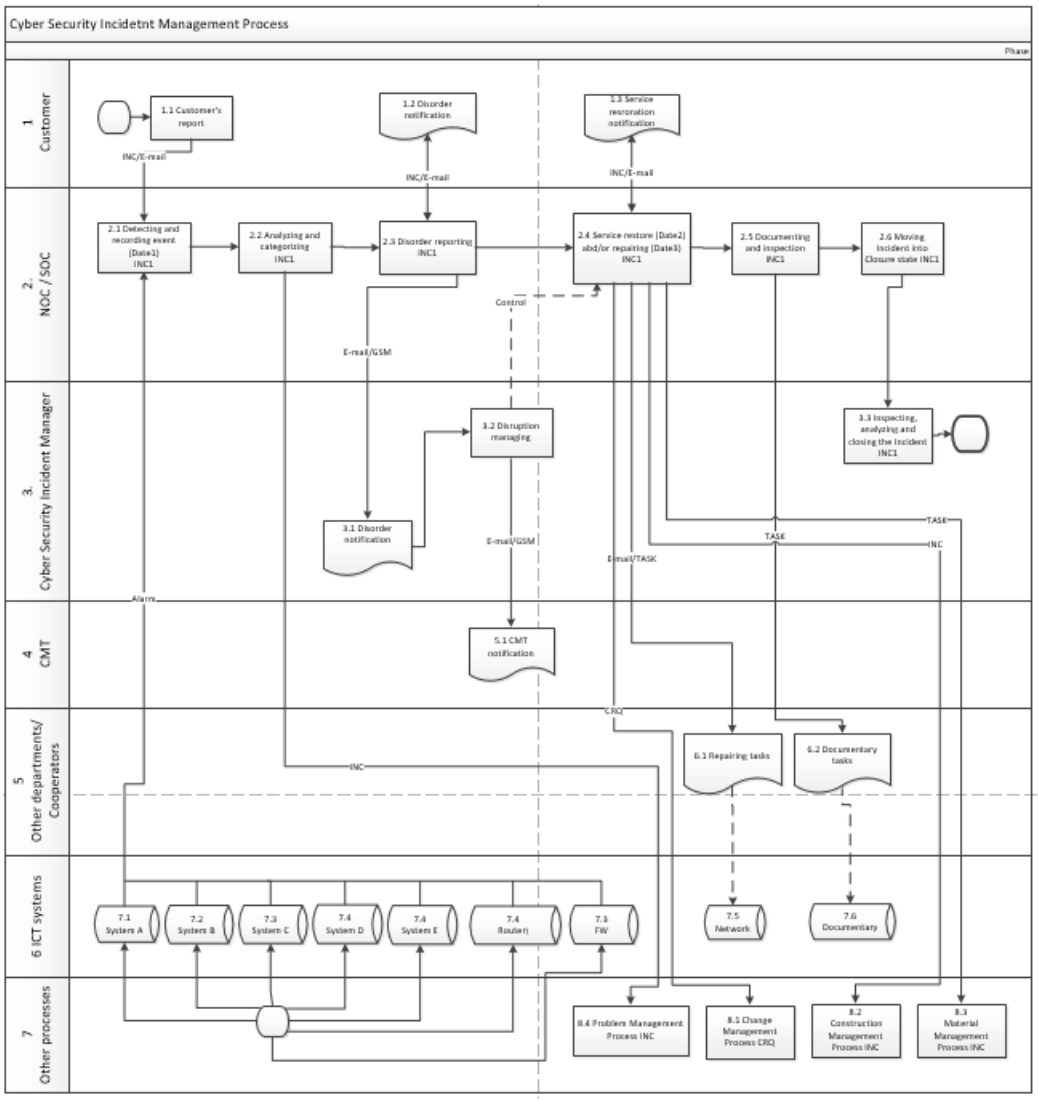


Figure 4. Flow Process Map Cyber Security Incident Management

### 4.2.1 Categorization of the Cyber Security Incident

One important purpose of the Cyber Security Incident Process is to enable the production of appropriate reports on the process. That means the measurement of the process itself, as well as the measurement wanted to achieve concerning the cyber incidents. Measuring the process is important for the continuous development for finding out any need for upgrading the process. Measuring the occurred cyber incident is important to identify the trends and by that recognizing the deviations referring to that acknowledgement.

First of all it had to be defined what the cyber incident is and how it differs from the so called regular incident that occurs in the network or ICT system. Truth is that the network incident and the cyber incident are concepts that partially overlap with each other, and there is no exact boundary between them. Somehow it had to be defined which events were identified as cyber incidents and this reflection resulted in Table 2. The Vocabulary of Cyber Security launched by The Security Committee and Sanastokeskus was used as a support when the categories were defined as well as the Incident Classification / Incident Taxonomy according to eCSIRT.net. (The Vocabulary of Cyber Security 2018, the Incident Classification / Incident Taxonomy according to eCSIRT.net 2012.)

Table 2. Categorizing Table

| Category | Description | Keywords |
|---|---|---|
| Test | Used in test and educational cases | practise, drill, test, rehearsal |
| DoS | Denial-of-Service attack that prevents or disturbs the use or limits the functionality of networks, systems or softwares by resource overload. Includes both source and destination of target. Attack can as well be exploited as a physical affection (DoS, DDoS, Sabotage) | Dos, DDoS, sabotage |
| Malware | Malware assembled successfully and affectin the system or software. | malware, virus, trojan, worm, spyware, dialler, rootkit, rat, ransomware |
| Inappropriate use | User does not follow the contrary to instructions. Wasting of resources. Junkmail. Inappropriate content (malicious, insulting, targeting to children, sexual, adoring violance) | fraud, spam, junkmail, abuse, sex, child, porn, violence |
| Reconnaissance | Intelligence gathering on information networks. Includes the activities which are executed for recognizing the open ports of systems, protocols, services or combinations of these for the aim of later intrusion. Reconnaissance can occur also by the methods of social hacking (Social Engineering), scanning, sniffing. | scanning, sniffing, social engineering, reconnaissance |
| Unauthorised access | Source of the unauthorized access may be revealed internally or as an outcome of burglary or attempt to hack from outside of the company. Attacker gets an access into a logical asset or a physical infrastructure such as: network, ICT-system or software, information or any other valuable resource without authorization. Copyright infringement. Login attempts. Bruteforce. Attempts to take advantage of vulnerability. | bot, botnet, copyright, bruteforce, access control, authentication, verification |
| Theft or disappearance | The information or the property has been stolen or lost. | lost, theft, steal |
| Vulnerability | Detected vulnerability for example in protection, activity or ICT system. | vulnerability |
| Unconfirment | An event that has not yet been confirmed as true. | unconfirment |
| Security breach | An incident concerning privacy protection. GDPR. | identity, gdpr, confidentality of personal information. |
| False positive | A finding that turns out to be a misinterpretation. | false positive, misinterpretation. |
| Other event | Used when other categories are not applicable. | |

The Risk Management Table served as the basis of cyber incident categorization. The categorization has different purposes and is closely linked to reporting. When categoriazation is generated properly, the reports will reflect the reality and therefore they are reliable. Categorization is divided on BMC Remedy into four different areas based on the functionality: Operational Categorization, Product Categorization, Resolution Categorization and Resolution Product Categorization. All the employees operating with the Cyber Security Incident Managemtn Process had to be trained how to categorize the incidents properly, which was one part of impelenting the process. Figure 5 shows how the categorization areas were defined in Erillisverkot Group. It is important to see that the function of Categorization fields can vary depending on the purpose of the company using it.

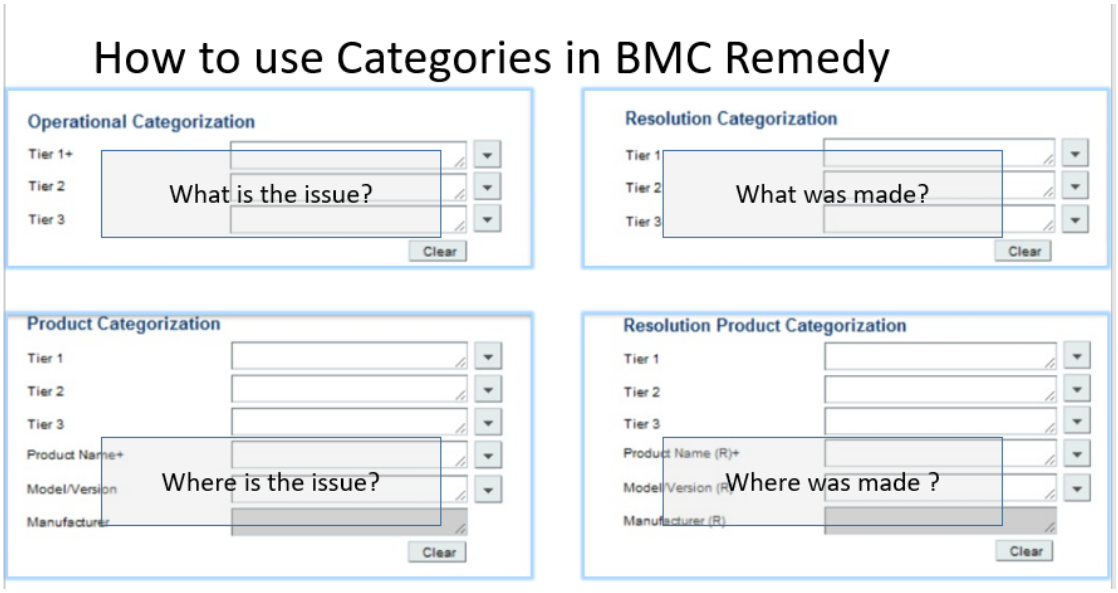


Figure 5. Categories in BMC Remedy

All categorizations have three levels, Tier 1, Tier 2 and Tier 3. When moving down on the tiers, the categorization becomes more specific and gives detailed information concerning the incident.

Operational Categorization answers the question What is the issue? In the Cyber Security Incident Management Process the Operational Categorization had the Tier 1. categories listed below:

- Inappropriate use
- Malware
- Reconnaissance
- Unauthorized access
- Dos
- Security breach
- Vulnerability
- Theft or disappearance
- Other
- Test

That categorization is based on the Risk Management and Threat Management and it is supposed to cover all operational types of cyber incidents expected to occur in Erillisverkot Group.

Product Categorization is supposed to inform what product or service the cyber incident affects. For that categorization it was a necessity to recognize Erillisverkot Group's main assets and give them a classification. Based on the classification and importance they were given a value from low to critical. The asset classification is seen on Table 3.

Table 3. Assets of Erillisverkot Group

| ERILLISVERKOT GROUP'S ASSETS AND VALUATION (BASED ON THE CRITICALITY) | | |
|---|---|---|
| ASSET | CLASSIFICATION | VALUE |
| Network | Primary asset, organizational, virtual | Critical |
| Ability to operate and monitor the networ | Supporting asset, organizational, virtua | High |
| Ability to build the network | Supporting asset, organizational, virtua | Critical |
| Signal stations | Primary asset, organizational, physical | High |
| Fibers | Primary asset, organizational, physical | Medium |
| Information | Supporting asset, organizational, physic | Critical |
| Key personnel | Supporting asset, organizational, physic | High |
| Network Operation Center | Supporting asset, organizational, physic | High |
| Reputation | Supporting asset, organizational, virtua | Medium |
| Image | Supporting asset, organizational, virtua | Medium |

These assets include all the products and services Erillisverkot Group produces and they can be found in the Product Categorization in BMC Remedy. As in all categorization areas in the Product Categorization the description of the product or service gets more detailed when descending the tiers (Tier 1 to 3).

The Resolution Categorization as well as the the Resolution Product Categorization is filled in the Cyber Security Incident ticket when the incident has been resolved. The Resolution Categorization answers the question What was made? The calssification needed to recognize common procedures used when the incidents were processed in Erillisverkot Group. These categorizations also become more specific when going further on the tiers mentioned before. For that categorization it was important to recognize the resources and functions Erillisverkot Group used while restoring services and fixing the problems occuring in the network environment.

In most cases the Resolution Product Categorization is similar to Product Categorization, however there may occur cases, when the disturbance is indicated in some product and the reason for that will be located in another product of service. For example, the network router may indicate a major alarm and after the case has been resolved, the reason for the router failure is located in the broken fiber cable.

### 4.2.2 Life Cycle of the Cyber Security Incident ticket in BMC Remedy

Input to the Cyber Security Incident Management Process can come in two different ways; either when the customer makes an announcement of disruption, or if a system alarm indicates a disruption. A customer makes an announcement by calling the NOC/SOC or by sending an email. After the input, the ticket into the BMC Remedy is not generated automatically. That is the cause of the high class of the network security in Erillisverkot Group, and therefore systems and networks from different security levels are not connected together, not physically further as logically. Security levels are the classified levels from Level IV to Level II, and these are explained more specifically in chapter 3.2.2. Katakri. So, when the input occurs the NOC/SOC operator generates the ticket into the BMC Remedy and fills all the required fields to the ticket.

The categorizations of the incident are evaluated regarding the information of the starting point, and time stamps are set as they are defined in the Cyber Security Incident Process Description.

Finally, when the case has been resolved and the ticket is closed, the Cyber Security Incident ticket has four different time stamps. The first time stamp is the date and time of generating the ticket, and it is called Submit Date. That time stamp originates automatically when the ticket has been created in the BMC Remedy system. On the Dates -tab there are also three date fields which have to be filled by the user, Date 1, Date 2 and Date 3 fields. Date 1 is the time when the disruption has started. Date 2 is the service restoration time and Date 3 is the time when the failure has been repaired. Date 2 and Date 3 are often similar; the service is restored many times at the same time as the malfunction is repared. Howerer, there are also many cases when the service restoration can be executed before the malfunction is even repaired. These kinds of incidents are cases when the service can be restored for example by re-routing the connection service uses. In that case the service uses so called protected route while the main route is unavailable. After the main connection or link has been repaired, the service will be returned to its main route. The

protection state of the service depends on its criticality and the SLA pre-agreed in the contract between the customer and the service provider.

The time between the Date 1 and Date 2 indicates the service restoration time, which is one important issue when the service restoration time is reported. Erillisverkot Group reports service restoration times to all its customers monthly so that the customers can be aware of whether the SLA is realised or not. Also, the time of repairing is measured and reported regularly. Repairing time is the time between the Date 1 and Date 3, from the startpoint of disruption to the time it is repaired. The quality of the technician team working inside Erillisverkot Group, as well as the quality of the technician teams cooperators use, is measured for finding out any decline or loss of quality.

The time between the Date 1 and the Submit Date indicates the react time, i.e. the time when the disruption occurs until the time when it has been noticed and the ticket of that particular incident has been created to the BMC Remedy system. That time is reported weekly inside Erillisverkot Group to find if there appears too much delay on the reaction time. If delay increases so that it surpasses a certain threshold, the Process Manager reports of it to the supervisor so the cause of delay can be investigated and eliminated further.

These reports mentioned above provide the information for Erillisverkot Group so that it has availability to recognize all the declines of its own, or the cooperators' quality of services. By recognizing the declines immediately or even as rapidly as possible, the improvements and strategies for developing the activity can be started.

Analysis and Categorization starts after the ticket has been created in the BMC Remedy and it goes through the lifecycle of the ticket if necessary. After the Cyber Security Incident has been categorized properly, it needs to be analyzed. Analyzing includes the analysis of the impacts and criticality concerning a particular event. After the analysis customers are informed by sending a disruption announcement via e-mail. The disruption announcement informs certain customers of what has happened, what services are affected, where and when the event occurred and, if possible, an estimated service restoration time is included into the announcement. If the cyber security incident is wide concerning the impact, or if it concerns critical

services of Erillisverkot Group, also the higher management is informed about that particular event. If the estimate of the service restoration is impossible, disrupt announcements are sent regularly every three hours since the first announcement until the service has been restored. This is the part of good quality of service Erillisverkot Group aims to provide.

Once the occurred event has been categorized, analyzed and the customers are informed, as well as the higher management if needed, the network operator starts the actions needed for service restoration. There is a possibility that the operator can repair the malfunction by himself/herself by performing the necessary operations and configurations in the network using remote access. If the operator can-not repair the malfunction remote, he/she creates a task which is attached in the ticket. The task works as a request for the level 2 specialist and/or for the technician team if necessary. All the actions the operator executes and every notification received from the customers, from another level specialists and/or from the technician team are written down in the tickets' Work Info field. If processing the ticket produces any documents, they are attached to the ticket.

After the necessary actions have been made, and the service is restored and the malfunction repaired, the NOC/SOC operator fills the final comments in the Resolution field of incident, adds final dates on the Date 2 and Date 3 field and informs the customers about the service restoration. The notifications in the Resolution field must show what was the root cause of the event and how it was resolved. If resolving the event requires changes in Erillisverkot Group's environment, the NOC/SOC operator generates an input to the department that upgrades all the necessary documents concerning that particular case.

The manager of the Incident Management Process checks out the ticket after the NOC/SOC operator has turned it into Resolved stage and if all the notifications are made appropriately, the manager turns the ticket into Closed stage. If that particular case generates needs for other processes, e.g. the Construction Management Process, Change Management Process, Problem Management Process or some other processess, the manager takes care of putting the input forward to another process.

## 4.3 Testing the process

In May 2019 the draft of the Cyber Incident Management Process was ready for testing. The process was reviewed in the laboratory environment of Erillisverkot Group using the same ICT system that is in the productive use in Erillisverkot Group. The reviewing was planned to be put into practice with few key persons of the process, so that every operator and functionality of the process was represented. The testing was accomplished in June 2019 and it took two working days.

The testing was executed with few cyber incidents, which were evaluated as probable and the most common cases. The goal was to find all inconsistencies and lacks of the process; every step was observed and the findings were written down and documented for later development of the process. The testing adduced if some descriptions were not clear enough for the operator to understand it, or if some steps were possibly completely missing. In addition, the testing gave the picture that the categorization is sufficient enough but does not contain any unnecessary categorizations.

Another goal of testing was to find out that the process produces all the needed indicators as required for the reporting and measurement. For that purpose there had to be so many test cases, that it was enough to produce reports which were reliable enough and represented the reality as well as possible.

After the draft of the Cyber Incident Management Process was tested, all documents produced during the testing were analyzed. These documents covered reports, recorded findings, and comments as well as feedback requested from the test participants related to the process. Based on the analysis, the necessary corrective actions were taken for the process description and the test was performed again. After testing, it was not found that the process description needed further modification; hence, it was determined that the process is ready to be transferred into production. In addition to identifying shortcomings in the process description during the process testing, a catalog of necessary refinement procedures was also produced. These guidelines are intended to serve as a more detailed descriptions in support of the process in more specific handling of some events.

In connection wih testing the process, certain key persons also received training in the process and its various functionalities, and some of them produced educational material to support the training of the rest personnel.

## 4.4 Process implementation in Erillisverkot Group

The results were analyzed by testing the process and all the necessary procedures included in it in a laboratory environment corresponding to Erillisverkot Group's production network as for the network topology and components. The pe rsons participated the testing were the ones who will be operating with the Cyber Security Incident Management Process in the future. The operations for improvement of the process were executed after demonstration and testing and after that the process was ready for the implementation.

The implementation of the Cyber Security Incident Process is a continuous project that involves training the employees operating with the process, upgrading every procedure and guideline when necessary, and reporting the results so the development targets are identified through sufficienly comprehensive reports.

The first step was to modify the system configuration of BMC Remedy to suit the process. That was executed by the specialist who is responsible of the BMC Remedy configuration. The specialist was given the criteria and the parameters according to the process plan for changing the configuration. That partiular configuration was earlier tested in the laboratory. After the configuration was modified the employees were trained in the operating models and procedures of the Cyber Security Incident Process. The content of the training was tailored to match the role of the employee in the process.

First and foremost, the training was introduced to employees to understand what the Cyber Security Incident Management Process is all about and how the process description appears in the flow chart. That means all the employees were expected to understand how to identify an event that is an input of the process, as well as the desired output of the process, and what all the procedures are that are needed to execute to reach the goal. Also, it was important that everyone recognized their own

role in the process and in what cases they were expected to give an input to another process or to another role in that particular process.

In addition, the training involved many different instructions for processing different kinds of cyber incidents. These instructions are more technical and specifical and require expert knowlegde from the operator. The overview of instructions generated during the process creation are described in the next chapter.

As said before, the implementation is not a one-time event but a continuing process where issues related to process development are regularly reviewed. This development work is a crucial part of Erillisverkot Group's larger development work concerning the whole process package, and where all the sub-processes are reviewed considered as a whole. The Cyber Security Incident Management Process became as a part of the one main process Maintenance of Network and Services and it is reviewed regularly from the different point of views. Once in a week is a review based on the weekly report, where the significant events are highlighted; once in a month when two different kinds of reports are produced, one concerning the cyber incidents and one concerning the process itself. Once in a year there is a bigger reviewing session where the sub-processes are reviewed regarding the main processes. Once in a month there is also a review where the customers are reported on events that had affected services provided to them. These tailored reports are a combination of the all sub-process reports under the Maintenance of Network and Services Process.

## 4.5 Overview of procedures and instructions originated during the process generation

Several instructions and guidelines were generated during the creation of the Cyber Security Incident Management Process. These documents describe and guide how the functions of the process are intended to execute. The most important documentation, of course, is the process description and the flow chart of the Cyber Security Incident Management Process. However, in addition, the process required several technical and detailed instructions almost for every kind of incident that can

be found in the categorization. These instructions are helping the employees who are operating in the process, especially in the orientation phase and after that they act as a support when a rarely recurring event occurs. In addition to the detailed instructions, plenty of training material was created during the process creation, which is intended for training and familiarlizing the necessary personnel with it during the implementation phase of the process.

Because the cyber security events are very broad concept and can cover a wide variety of events involving both physical and logical environments, in addition to a top-level process description, a large amount of case-specific guidance had to be produced. The instructions produced relate e.g. to fault reporting, BMC Remedy operations, detailed handling of various events, various systems such as power supply systems, transmission systems, data systems, etc. In addition, instructions were produced related to personnel safety and facility safety. Fault reporting includes the fault reporting in the direction of the management of Erillisverkot Group and in the customer interface. The content of the fault messages is precisely defined in the instruction and must comply with the safety regulations for classified information (KATAKRI). BMC Remedy guidelines instruct a ticket is handled in the system throughout its lifecycle. The guide defines which fields must be filled in and which parameters must be found on the ticket. These are important for reporting so that the measurement results are reliable.

# 5 Conclusions

Generating the draft of Cyber Incident Management Process started in the autumn of 2018. During the spring of 2018, the structure for that particular process was generated, and the result was a process flowchart which is the basis for configuring the systems to correspond the process as required.

The process demonstration was arranged during the summer of 2019 in the laboratory environment, and in autumn of 2019 the report of the process was generated. Implementing the process in Erillisverkot Group has been continued since autumn of 2019 when also the CSIRT Group was established.

The resources for the execution the thesis were allocated by Erillisverkot Group including e.g. the necessary support from different technology specialists, travelling costs, laboratory environment as well as all the required components and recourses for demonstration.

The biggest challenge was to describe each step of the process so that it is clear and univocal enough so that the one, who follows it, could not understand it wrong, and the result would be as required for the moving to the next step in the process description. Another challenge was to describe all the steps so that they matched every incident of that particular process. That means the description must be generic enough to avoid several descriptions for each detailed incident. These two points where inverse to each other; if the description is too detailed, the lack of generic information may become apparent, and if the description is too generic, the risk of misunderstanding increases. Therefore, it is important to find a balance between these two issues so that the description is sufficient enough.

Another big challenge is the high security level of Erillisverkot Group. The high level of security extends to almost every component inside Erillisverkot Group, such as the ICT systems and networks the organization uses and even to the internal information sharing between the different departments of Erillisverkot Group. Because the networks and the ICT systems at different levels of security are not connected to each other, not even physically. This causes great amount of manual work for example when processing incidents, which means the information must be transferred manually from one system or network to another. This in turn increases the possibility of errors in the data.

One challenge was involved in the fact that the BMC Remedy is used in every processe Erillisverkot Group runs, and all different processes have different purposes. That means the categorizations and the functions of different fields in BMC Remedy are used for very different purposes, and it was important to consider the needs of all other processes while planning the Cyber Security Incident Management Process. This also posed challenges during the process implementation so that every process operator defines the right categorizations they are supposed to use.

The main goal was to generate the Cyber Security Incident Management Process for Erillisverkot Group, including all necessary components, such as the flow chart, technical descriptions, categorization and classification models, instructions and guidelines for the ones operating with the process and report basis for producing appropriate reports. After the process description was generated and the process was tested, the main goal could be considered achieved. The Cyber Security Incident Management Process seemed to produce all necessary incicators concerning reporting and measuring the process itself as well as the trends of cyber incidents that may occur in Erillisverkot Group. These reports are the main tools concerning the continious development of the process as well as the prepareness for the cyber threats and protectioning all the functionalities of Erillisverkot Group.

The research was successfully scheduled according to the goals of Erillisverkot Group, and the Cyber Security Incident Management Process was implemented as it was intended. Instead, the Master's Thesis Report schedule was much more longer than it was originally planned. The reason for that was the amount of work according to the generating the process alongside other tasks, and there were little time and resources left for producing Master's Thesis at the same time. After the process was at a stage that it could be implemented in Erillisverkot Group, the implentation itself took plenty of energy and time. On top of all that, in the spring of 2020 the world was shaken by a dangerous virus that caused Erillisverkot Group to be declared under a state of emergency, which further delayed the completion of this Master's Thesis. Reflecting on the above, the results of the reseach were achieved better than expected.

## References

Groppe, K. 2019. *Blog writing in Healthcare Information and Management Systems Society*. Accessed on 13 September 2019. Retrieved from https://www.himss.org/news/three-ways-improve-your-security-incident-response-plan

Mueller, R. 2012. *Speech of III Director Federal Bureau of Investigation*. March 01, 2012. Accessed on 6 May 2019. Retrieved from https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Laamanen, K., & Tinnilä, M. 2009. *Prosessijohtamisen käsitteet.Terms and concepts in business process management.* Espoo: Teknologiateollisuus Oy.

*ITIL Foundation, ITIL 4 edition*. 2019. Glossary. Axelos Global Best Practice. Accessed on 10 November 2019. Retrieved from https://purplegriffon.com/downloads/resources/itil4-foundation-glossary-january-2019.pdf

*Manage Engine.* 2019. The definitive guide to ITIL incident management. Zoho Corp. Accessed on 12 December 2019. Retrieved from https://www.manageengine.com/products/service-desk/itil-incident-management-guide.html#def

*NIST History*. 2002. Page on NIST Institution website. Accessed on 24. April 2020. Retrieved from https://www.nist.gov/history

*NIST Cyber Security Framework*. 2020. Page on NIST Institution website. Accessed on 24. April 2020. Retrieved from https://www.nist.gov/cyberframework

*Framework for Improving Critical Infrastructure Cybersecurity.* 2018. Document published by the National Institute of Standards and Technoly. 16. April 2018. Accessed on 24. April 2020. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

*BMC Corporation*. 2020. Page on BMC Corporation website. Accessed on 24. April 2020. Retrieved from https://www.bmc.com/corporate/about-bmc-software.html

*BMC IT-solutions*. 2020. Page on BMC Corporation website. Accessed on 24. April 2020. Retrieved from https://www.bmc.com/it-solutions/remedy-itsm.html

*Erillisverkot Group*. 2020. Page on Erillisverkot Group website. Accessed on 15 September 2020. Retrieved from https://www.erillisverkot.fi/en

*The Advisory Committee on Information Management in Public Administration*. 2010. Page on the Finnish Government website. Accessed on 2 January 2020. Retrieved from https://valtioneuvosto.fi/en/project?tunnus=VM007:00/2010

*JHS-Public Administration Recommendations*. 2012. JUHTA-Advisory Committee on Information Management in Public Administration. Accessed on 2 January 2020. Retrieved from http://www.jhs-suositukset.fi/suomi/jhs152

*Tietoturvallisuuden auditointityökalun (Katakri) uudistus on valmis*. 2015. Document published by the Finnish Government. Ministry of Defense. Accessed on 2 January 2020. Retrieved from https://valtioneuvosto.fi/artikkeli/-/asset_publisher/tietoturvallisuuden-auditointityokalun-katakri-uudistus-on-valmis

*National Security Auditing Criteria (KATAKRI) version II*. 2011. Document published by the Ministry of Defence. Accessed on 2 January 2020. Retrieved from https://www.defmin.fi/files/1871/KATAKRI_eng_version.pdf

*The Vocabulary of Cyber Security*. 2018. Document published by The Security Committee. Accessed on April 10. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

*Incident Classification / Incident Taxonomy according to eCSIRT.net*. 2012. Document published by S-CURE bv, PRESECURE GmbH and SURFnet bv. Accessed on April 10 2020. Retrieved from https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

# Appendix 1. Basic Information Form

## Code of conduct of the Cyber Security Incident Management Process

## Basic information form (following the JHS 152 recommendation)

This basic information form should be prepared for each identified and described process. The process is mainly described with a floating path diagram (MS Visio) and a textual functions table (MS Word) that describes the operations described in it in more detail. In certain cases, it is more appropriate to describe the process as an annual clock rather than a floating path diagram. In this case, both the year clock and the complementary operations section are described in the same file (MS Power Point). The aim is to make the description unambiguous and comprehensible so that everyone involved in the process understands the described instruction in the same way. The description should correspond to the actual operation.

| | | |
|---|---|---|
| 1 | Instruction name | The Cyber Security Incident Management Process |
| 2 | Author and date of the description | Tanja Ruskojärvi 13.8.2019 |
| 3 | Acceptance of the description into the process entity; acceptor and date | |
| 4 | Version | 1.2 |
| 5 | The purpose of the process | The process handles the Erillisverkot Group's cyber security events, which are operations related to the maintenance of the delivered infrastructure or network service or network based cyber events. |
| 6 | Owner of the process | Pekka Kuittinen |
| 7 | Process modeler and the date of modeling | |
| 8 | Process input | Customer's notification or system alarm |
| 9 | Process output | Processing the transactions so that the situation after the incident corresponds to the product ordered by the customer or the network corresponds to the situation that existed before the start of the event. |
| 10 | Process customers | Public authorities and commercial operators using infrastructure or network services of Erillisverkot Group |

| | | |
|---|---|---|
| 11 | Process stakeholders | Documentalist: makes the final documents, design of classified information<br><br>Products and Services Department: priority of stations, contracts, software, service agreements with customers, agreements with commercial operators<br><br>Technician Department: Repairing and scheduled maintenance<br><br>Administrative building department: Property maintenance and upkeep<br><br>Cable contractor: Cable network repair |
| 12 | Process customers' needs and requirements | Functionality if network services provided to customers in accordance with service agreements. |
| 13 | Process success factors | Documented production environment, described network services, skilled employees, functioning management system. |
| 14 | Process metrics | Cyber Incident Management metrics |
| 15 | Process key resources and other volume information | Personnel of the Operation and maintenance department |
| 16 | Process control and development procedure | Monthly reports, weekly reports, customer reports and steering group of the Operation and maintenance department |
| 17 | Interfaces to other processes | Inputs to the **Problem Management Process** to determine the root causes of events.<br><br>Inputs to the **Support Service Process** to develop cybersecurity and personnel security.<br><br>Inputs to the **Construction and Supply Management Process** to make necessary investments.<br><br>Requests for the **Material Management Process** to allocate spare parts and spare devices needed to replace defective ones. |

# Appendix 2. Cyber Security Management Process Operating Procedures

## Cyber Security Management Process

## Operating procedures

| 1. Customer | | | |
|---|---|---|---|
| Number | Function | Operation | Output |
| 1.1 | Customer's report | The customer prepares a report of the detected cyber deviation or service deviation, or a service request for the operation concerning maintenance. | Customer reports of the deviation or makes the service request either to the BMC Remedy or via E-mail (depending on customer) |
| 1.2 | Customer receives a fault message | Fault is reported according to the fault-reporting model. | The fault reporting is provided by the BMC Remedy or via E-mail (depending on customer) |
| 1.3 | Customer receives a service restoration notification | Fault is reported according to the fault-reporting model. | The fault reporting is provided by the BMC Remedy or via E-mail (depending on customer) |

| **2. NOC / SOC** | | | |
|---|---|---|---|
| Number | Function | Operation | Output |
| 2.1 | Detecting and recording the event | NOC/SOC receives the customer's report of deviation, or the customer's service request prepared in step 1.1. Or the event input comes from the system management environment (system alarm).<br><br>The incident is created in the BMC Remedy based on the input. | NOC / SOC receives input from the event.<br><br>If the input comes on media other than BMC Remedy, a new incident is created. |
| 2.2 | Analyzing, prioritization and categorizing the event | NOC/SOC analyzes the input and classifies the incident according to the event's effectiveness, functionality and technology. Priority is determined by the impact of the event. The customer effects of an event are also defined at this stage. If the event causes security deviation, a security deviation incident is created. | Event analysis, classification and customer impact are defined. The security deviation incident is created if the conditions are met. |
| 2.3 | Fault reporting | Fault is reported according to the fault-reporting model. | Disorder notification is prepared for customers if the event affects the online services provided to customers.<br><br>Inform the Cyber Security Incident |

| | | | |
|---|---|---|---|
| | | | Manager in accordance with the management fault reporting model. |
| 2.4 | Service restoration and/or repairing | Under the leadership of the NOC/SOC actions are performed in accordance with the event of service request. The aim is to return the provided services as soon as possible, albeit using a temporary solution. The goal is to reach the state that existed before the event occurred.<br><br>Repairing actions continue after the service restoration if necessary.<br><br>If repair of the defect requires decisions to accept the costs associated with the repair, then the manager shall make such decisions as necessary, excluding investment decisions.<br><br>Partners and stakeholders can be used to restore the situation to the pre-event state. | NOC /SOC manages and implements restoration to the pre-event state. |
| 2.5 | Documentation and inspection | Managing the documentation work as required by the event and checking the degree of readiness of the work.<br><br>Once the documentation is complete, the actions caused by the event are checked and it is ensured that the event is ready to close. | Manage the documentation work required by the event and check the degree of readiness of the work.<br><br>An input (task) to the documentation producer |

| | | | |
|---|---|---|---|
| | | | for the documentation. |
| 2.6 | The incident is moved to Closure state | NOC/SOC suggests to management that the event can be closed. | NOC/SOC switches the incident to closure state. |

| **3. Cyber Security Incident Manager** | | | |
|---|---|---|---|
| Number | Function | Operation | Output |
| 3.1 | The Cyber Incident Manager receives a fault message | Fault reporting is executed according to the fault-reporting model. | The fault is reported by appropriate medium (phone, E-mail, collaboration instruments) |
| 3.2 | Disruption managing | If the impact of the event is classified as critical, the Cyber Security Incident Manager is responsible for managing the situation. | Management of corrective actions, making decisions and informing management. |
| 3.3 | Inspecting, analyzing and closing the incident | The Cyber Security Incident Manager inspects the work package and closes the incident. | Event work info, entries and documentation are checked and the incident is closed when everything is found to be ready. |

| **4. CMT** | | | |
|---|---|---|---|
| Number | Function | Operation | Output |
| 4.1 | CMT receives a fault message | Fault reporting is executed according to the fault-reporting model.<br><br>CMT takes action according to the level of interference. | The fault reporting via E-mail. |

| **5. Other departments / cooperators** | | | |
|---|---|---|---|
| Number | Function | Operation | Output |
| 5.1 | Repairing tasks | The resources used for repairing and service restoration receive input for completing the work. | Receives task as a work order. |
| 5.2 | Documentary tasks | The resources used for documentation receive input on how to complete the documentation work. | Receives task as a work order |

| **6. ICT systems** | | | |
|---|---|---|---|
| Number | Function | Operation | Output |
| 6.1 | System management | Network technology<br>Systems (without mentioning vendors):<br>- Transmission systems and equipment<br>- MPLS routers, CE devices<br>- Firewalls<br>- Security technology equipment<br>- All other infrastructure | System alarms from the network management system |
| 6.2 | Network | Network technology<br>Systems (without mentioning vendors):<br>- Transmission systems and equipment<br>- MPLS routers, CE devices<br>- Firewalls<br>- Security technology equipment | Device configuration |

| | | | |
|---|---|---|---|
| | | - All other infrastructure | |
| 6.3 | Documentation | Maintained documents | Changes to documentation |

| **7. Other processes** | | | |
|---|---|---|---|
| Number | Function | Operation | Output |
| 7.1 | Change Management Process | Management of production network changes and downtime | An input (task) to Change Management Process |
| 7.2 | Construction Management Process | When the measures of the event require investments or changes in the structures of the production network, a request for these is created for the Network Design Department. | An input (task) to Construction Management Process |
| 7.3 | Material Management Process | Ordering material. | An input (task) to Material Management Process |
| 7.4 | Problem Management Process | If the event is recurring or requires a more detailed explanation of the root cause, an input is made to the Problem Management Process. | An input (task) to Problem Management Process |

# Appendix 3. Flow Chart